MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2017/2018

TPB3141 – PASSWORD AUTHENTICATION AND BIOMETRICS

(All sections / Groups)

23 OCTOBER 2017
9.00 a.m – 11.00 a.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 7 pages, excluding the cover page, with 5 questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

Question 1:

Please attempt **ALL** multiple choice questions. [12 marks]

1. Which of the following is the characteristic of a strong password?
   a. Include numerical characters only
   b. Contain symbol characters only
   c. Can be used only a certain number of days
   d. Password composed of character strings from the username

2. _______ provides users with a stable and secure device to regulate network log-on using a dynamic password.
   a. Digital certificate
   b. Storage token
   c. Dynamic token
   d. Password synchronization

3. Which of the following is NOT TRUE about digital certificates and PKI?
   a. Allow users of an unsecured public network to securely and privately exchange data.
   b. Public key is something that you make public. It is freely distributed and can be seen by all users.
   c. Use a dynamic cryptographic key to verify the identity of the sender.
   d. A registration authority acts as the verifier for the certificate authority before a digital certificate is issued to a requestor

4. _________ is the process by which biometric features of the sample are selected or enhanced. Typically, this process relies on a set of algorithms, and the method varies depending on the type of biometric identification used.
   a. Matching
   b. Capture
   c. Feature extraction
   d. Recognition

Continued ....

5. _________ is a method of fooling a biometric identification management system, where an artificial object (like a fingerprint mold made of silicon) is presented to the biometric scanner that imitates the unique biological properties of a person which the system is designed to measure, so that the system will not be able to distinguish the artifact from the real biological target.
   a. Threat
   b. Mimic
   c. Spoofing
   d. Skimming

6. ________ is the most acceptable biometrics that we used daily to identify a person.
   a. Thumbprint biometrics
   b. Fingerprint biometrics
   c. Face biometrics
   d. Signature biometrics

7. _________-based biometrics is the field of study related to the measure of uniquely identifying and measurable patterns in human activities.
   a. Behavioral
   b. Psychological
   c. Physiological
   d. Psychosomatically

8. _________ is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology.
   a. Kerberos
   b. Anti-virus
   c. Firewall
   d. Single Sign On

9. In biometrics and forensic science, __________ are major features of a fingerprint, using which comparisons of one print with another can be made..
   a. minutiae
   b. delta points
   c. core points
   d. ridge

Continued ....

10. The _________ is any pocket-sized card that has embedded integrated circuits or, with a built-in microprocessor, used typically for electronic processes such as financial transactions and personal identification. E.g.: __________.
    a. smart cards; CIMB VISA payWave
    b. smart cards; Jusco memory card
    c. biometrics; Malaysian IC
    d. OTP Generator; HSBC Dynamic Token

11. The _________ relates to unauthorized collection, storage, and usage of biometric information.
    a. informational privacy
    b. personal privacy
    c. communication privacy
    d. digital privacy

12. The _________ is to be used within organizations to formulate security requirements and objectives.
    a. ISO/IEC 27001
    b. ISO 17799
    c. Private Communication Technology
    d. Secure Electronic Transaction

Continued ....

Question 2:

a) Fill in the blanks with the most appropriate card technology:

i. _________: Use a technology similar to the one used for music CDs or CD ROMS.

ii. _________: Contains only memory and it is mainly used to store information.

iii. _________: Contains memory together with a microprocessor. It has ability to make decisions about the data stored on the card.

iv. _________: A type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card.

v. _________: It is designed to deliberately reflect the source radio frequency (RF) in sequences that are interpreted as information in the form of digital data.

[5 marks]

b) The Internet of Things (IoT) is already making an impact on home automation and energy management systems, but many IoT sensors are placed in locations where power outlets are not conveniently located, forcing the sensors to run on battery power. On top of device authentication, if you want to ensure all passive IoT devices are able to receive energy via a radio frequency (RF) carrier wave which transmitted by an active WiFi power source;

i. What is the best technology to consider?

[1 mark]

ii. Justify your answer/ choice above with **FOUR [4]** supporting facts.

[4 marks]

c) Provide **TWO [2]** advantages of biometric-based authentication system when compared to the conventional password-based and token-based authentication systems.

[2 marks]

Continued ....

Question 3:

a) Refer to the table of password composition rule below, it is almost impossible to brute force a lengthy and complicated password.

Time to brute force password space, assuming 10,000 attempts per second			
Length of Characters	Lowercase (26 letters)	Uppercase, lowercase, digits (62 characters)	Uppercase, lowercase, digits, punctuation (94 characters)
5	19 minutes	1 day	8 days
6	8 hours	65 days	2 years
7	9 days	11 years	200 years
8	241 days	692 years	19,000 years
9	17 years	42,000 years	1.8 million years

i. Do you agree on this statement? Justify your answer.

[3 marks]

ii. Propose **TWO [2]** strategies to reduce the risk of this attack.

[2 marks]

b) Faculty of Information Science and Technology (FIST) deployed a fingerprint door access system in the faculty's pantry room, and only the authorized person – FIST staff can access to this room.

i. Differentiate the false acceptance rate (FAR) and false rejection rate (FRR) in a biometric solution. Explain them in this scenario.

[3 marks]

ii. Investigate **TWO [2]** possible causes which will greatly affect the FAR and FRR in this scenario. Justify your answer.

[4 marks]

Continued ....

Question 4:

a) The Malaysian government is installing 300 facial recognition devices to scan travelers entering and exiting the country at key entry points by the end of 2017, according to a report by Malay Mail Online. The facial recognition device would serve as an added security feature in addition to the thumbprint scanning devices that are already installed at the electronic gates. Travelers would scan their thumbprint as the facial recognition system scans their face, which would then be cross-checked with data embedded in the traveler's passport.

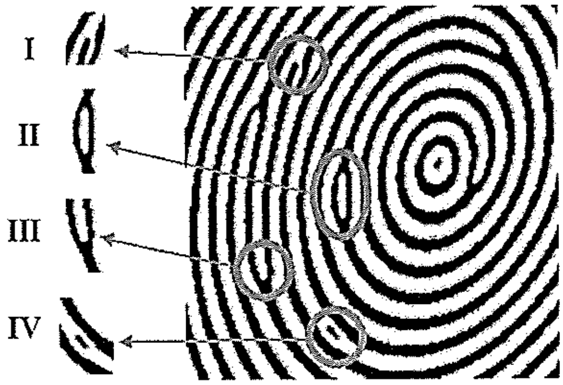
Evaluate the strengths of this deployment. You may discuss your opinions by comparing this deployment to other types of authentication method.

[5 marks]

b) Based on Bioprivacy Technology Risk Rating, study and rate the privacy risks of adopting voice, hand geometry and keystroke in the application of biometric applications. Table your findings.

[3 marks]

c) Given a fingerprint figure below, identify the components of I, II, III, and IV based on a given set of fingerprint ridge characteristics: [*delta; core; island; ridge ending; crossover; bifurcation; pore; ridge dot; ridge enclosure*].



[4 marks]

Continued ......

Question 5:

a) TSB is set to introduce iris recognition to its mobile banking app. It is the first bank in Europe to commit to providing the technology, as the Bank's high-tech experimentation speeds up. Customers with a Samsung Galaxy S8 or S8+ smartphone will be able to unlock their TSB mobile banking app using the Samsung Pass iris scanner. This means TSB's customers can access their banking using either the fingerprint (an existing feature) or the iris scanner.

Do you think iris is a reliable biometric modal? Justify your answer by discussing **FOUR [4]** distinctive features of iris biometrics.

[5 marks]

b) HHSB bank wants to provide a voice access banking, where the customers can use their voice to access all of their information, such as checking balance, search for a debit by check number or dollar amount, transfer funds between accounts and much more. Leveraging the telephony system, you are hired to develop a voice-based authentication system.

Illustrate and explain how a voice authentication works.

[6 marks]

c) Provide **TWO [2]** protocols which have been developed for Private Communication Technology.

[1 mark]

End of Page